Office of the Chief Information Officer/G-6

SHAPING THE ARMY NETWORK:

Mobile Technology

April 2017

CIO/G-6
ENABLING SUCCESS For Today and Tomorrow

U.S.ARMY

CIOG6.ARMY.MIL

DISCLAIMER

The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement.

CHANGES

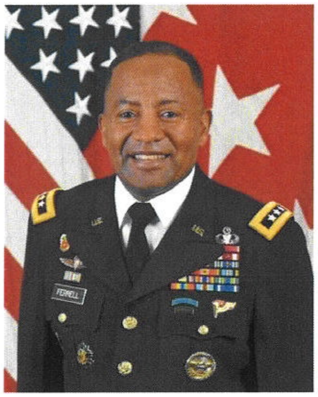
Refer requests for all changes that affect this document to:

Defensive Cyber Operations and Integration Division
CIO/G-6, ATTN: SAIS-CBB
107 Army Pentagon
Washington, DC 20310-0107

Table of Contents

This page intentionally left blank.

Executive Summary



The Army must embrace commercially available mobile technologies to become more dynamic, flexible, resilient, and capable of supporting user demand for data. Mobile technologies are not limited to smart phones; rather, they include sensors, applications, handheld devices, robotics, and wearables that will improve the speed and effectiveness of business and operational services, and drive innovation and demand for new capabilities. Using mobile technologies, doctors treat Soldiers remotely, engineers use 3-Dimensional (3D) printing to make emergency repairs to infrastructure, and commanders in smart command posts use sensor data from soldiers' uniforms, unmanned aerial and ground vehicles, and robots to make critical combat decisions.

This document sets a view where the Army will benefit from the explosion in commercial mobile technology. To date, the Army has not been aggressive enough at adopting mobile technologies. That changes now.

The Army will adopt new, commercially available mobile technologies in a matter of months, not years. Mobile technologies will be rapidly certified and mobile applications will operate using open architectures and standards. Innovative solutions to address cybersecurity risk will be employed. Through enhanced knowledge and situational awareness gained by using sensors and devices that leverage the cloud, the internet of things (IoT), and enterprise-wide data, our Soldiers and Civilians will enjoy improved security, health, and mission effectiveness everywhere, regardless of platform, location, or classification environment.

In accordance with the Mobile Technology end state defined herein, the Army must pursue three strategic goals with two guiding principles:

Goal 1: Establish a Mobile-Enabled Environment
Goal 2: Provide a Secure, Enterprise-wide Mobile Architecture
Goal 3: Accelerate Mobile Technology Adoption
Principle 1: Embrace commercial mobile technologies while using innovative solutions to reduce risk
Principle 2: Balance acceptable risk with the transformational benefits of mobile technology

First, the establishment of an Army Mobile Technology Partnership with Industry to drive Army-wide mobile initiatives towards achieving the Army Mobile Technology End State. This Partnership will prioritize the most impactful technologies, and collaborate with top researchers to meet the Army's future mobile technology and security needs. Second, a secure mobile architecture that will enable the use of mobile technologies. Third, the establishment of a Mobile Approved Products List (MAPL) to ensure that our Soldiers and Civilians can obtain Army-approved state-of-the-art mobile technologies as quickly as possible.

By achieving the Mobile Technology End State identified herein, the Army will enable all members of the Army community to perform their missions more effectively than ever before.

Robert S. Ferrell
Lieutenant General
Chief Information Officer/G-6

This page intentionally left blank.

Introduction

The explosion of mobile information technology (IT) is transforming IT delivery in the commercial sector with mobile devices and context-aware mobile apps shifting innovation and control to the edge, and empowering employees to serve customers better. Gartner expects that 60% of all business processes will be optimized for mobile technologies by 2020.[1] Mobile technologies are not limited to smart phones; rather, they include sensors, applications, handheld devices, robotics, and wearables that will improve the speed and effectiveness of business and operational services, and drive innovation and demand for new capabilities.

The Internet of Things (IoT) is one of the most significant technology trends, introducing the integration of digital sensing, computing, and communications capabilities. The digital shift to cloud, mobile, and leveraging IoT will be powerful forces behind business transformation. These technologies can augment current capabilities and services and foster innovation. Rapid app development will play a key role. Network and bandwidth costs will continue to drive users to favor apps that use the power and storage of the client device, and the cloud will be the default for scalable, self-service computing. Apps will be developed to support synchronized use of multiple devices: multiple screens, wearables, and other display devices (e.g. Ubuntu Touch). Machine-to-machine communications will support vast deployments of autonomous systems. Fifth Generation Networks (5G) will enable greater capacity to allow more devices to be connected, and lower energy requirements will extend device battery lives to more than 10 times what we see today. Cloud-based analytics will make sense of the information collected, creating the knowledge to support predictive and enhanced decision making.

Smart environments and smart platforms will be interconnected, resulting in enhanced intelligence and the following capability improvements, as highlighted by several Army stakeholders:

- **Predictive planning**. Sensor-driven analytics are used to enhance operational effectiveness. Data collected from sensors provide context-aware intelligence to anticipate future needs and provide autonomous responses.
- **Resource optimization**. Sensor-driven analytics are used to enhance command post logistics planning and operations to reduce fuel, water and waste.
- **Safety and well-being monitoring**. Wearable sensors monitor the well-being (stress, health, etc.) and safety of employees, provide full personnel accountability in case of emergency, particularly for Civilians working in the field and remote offices.
- **Untethered medical delivery**. IoT-enabled medical equipment allows clinicians and care providers to work and still have access to the data that they need, such as real-time battlefield triage data, patient records, Magnetic Resonance Imagery or X-ray images.
- **Robotics and autonomous surveillance**. Autonomous vehicles, unmanned aerial vehicles (UAVs) and unmanned ground vehicles (UGVs) perform site surveys and capture photos to provide intelligence. Publicly available information and social media, such as Facebook and Twitter, are used to increase sensor converge and provide early warnings.
- **Full office experience from any mobile devices, from anywhere**. Individuals can use enterprise-wide suites of business apps (Office 365, Google Apps, etc.) to perform their jobs from anywhere, from any device, so they are not tied to a desktop environment. Network-

[1] See http://www.gartner.com/smarterwithgartner/the-internet-of-things-is-a-revolution-waiting-to-happen/.

enabled devices such as printers and projectors are used to provide a paperless, smart environment that reduces workload, improves operations, unifies communication and makes users more effective.

- **Personal/business data synchronization**. Information (Such as calendars) is synchronized between government issued and personal devices.
- **Mobile-enabled enterprise self-services.** Mobile apps are expanded to include the full range of enterprise services, such as Human Resources (HR), finance, training and logistics.
- **Big Data Analytics -** Complex sensing and decision-making feedback by big data analytics assess the vast new sources of data provided by enhanced sensors.

The government (including the Army) has been a slow adopter of mobile technologies while the consumer and commercial markets have quickly adopted these technologies and revolutionized the way we live. The Army's adoption challenges include security and privacy as well as a lengthy accreditation and procurement process. To keep pace in a rapidly evolving market, the Army needs a more efficient process for identifying and deploying emerging mobile technologies. The Army has supported several mobile pilots, but it has struggled to move from pilot to implementation primarily due to the absence of a comprehensive Army approach to mobile capabilities.

Technological trends, opportunities, and threats compel the need for Army Mobile Technology guidance. Technological advances that have the potential to benefit the Army continue at a rapid pace. Soldiers are often early adopters of rapidly changing technologies. These Soldiers can identify novel ways to incorporate technology in support of Army operations. Stakeholders across the Army will be engaged to identify crucial mobile use cases that will impact future mission success. In addition, the Army's adversaries are increasingly more technologically savvy. Enemies will certainly continue to combine conventional and unconventional tactics to counter U.S. advantages in communications and mobile technologies. The Army must establish and sustain a mobile advantage.

This document serves as guidance to provoke thought and a means to inform and shape research, development and experimentation by both government and industry entities to ensure that the Army maintains a technology edge in future conflict. The necessary near-term activities to enable the Army to move towards the desired end state are identified herein. Subsequent guidance will identify lead Army organizations for the key activities identified in this document. As technology evolves and future threats emerge this end state will be adjusted.

Army Mobile Technology End State

End State

The Army will rapidly obtain commercial mobile technologies approved for use in a matter of months, not years, enabling users to benefit from enhanced knowledge and situational awareness, security, and mission effectiveness regardless of platform, location, or data classification.

This end state articulates the future environment in which the entire Army benefits from efficient deployment and use of mobile technologies. The goals, objectives, and associated key activities that are necessary to successfully achieve the Army Mobile Technology End State are defined below.

Guiding Principles

Two guiding principles shape the Army Mobile Technology goals and objectives. These principles should be communicated clearly and consistently when implementing and measuring progress towards the strategic objectives:

1. Embrace commercial mobile technologies while using innovative solutions to reduce risk.

The value of commercial mobile technologies will be felt across the Army, and will enable the Army to respond more quickly and more effectively to all current and emergent missions.

2. Balance acceptable risk with the transformational benefits of mobile technology.

The Army's success depends on our ability and capacity to adapt emerging technologies to the most pressing operational requirements, while simultaneously enabling those technologies across the full spectrum of Army missions. We must clearly articulate the benefits and acceptable risks to include cybersecurity risks associated with the implementation of any new technologies. To succeed, the Army must implement a risk assessment methodology. The risk assessment must account for anticipated future cyber threats.

Synchronization with Other Strategic Documents

Cloud computing, mobile computing, and data analytics are converging technologies that have critical dependencies on the network to provide the persistent connectivity and scalable bandwidth required by mobile users. The Army Network Campaign Plan, the Army Cloud Computing Strategy, and the Army Data Strategy, collectively with this document, provide a unified path forward for the Army to achieve the advantages of these technologies.

- The *Army Network Campaign Plan* establishes the criteria for a secure, integrated, standards-based environment that ensures uninterrupted global access for regionally aligned forces, unified action partners, supports the full range of military and business operations, and extends LandWarNet down to mobile devices.
- The *Army Cloud Strategy* strives to maintain a strategic and tactical advantage over adversaries through information dominance while determining the most appropriate cloud service and deployment model for migrating and improving secure mobile computing capabilities.
- The *Army Data Strategy* enables Mission Command to obtain and sustain a decisive operational advantage. The networked force requires the right data, at the right time, at the right place, limited only by policy and not by technology, leveraging mobile technologies as a critical element of that future environment.

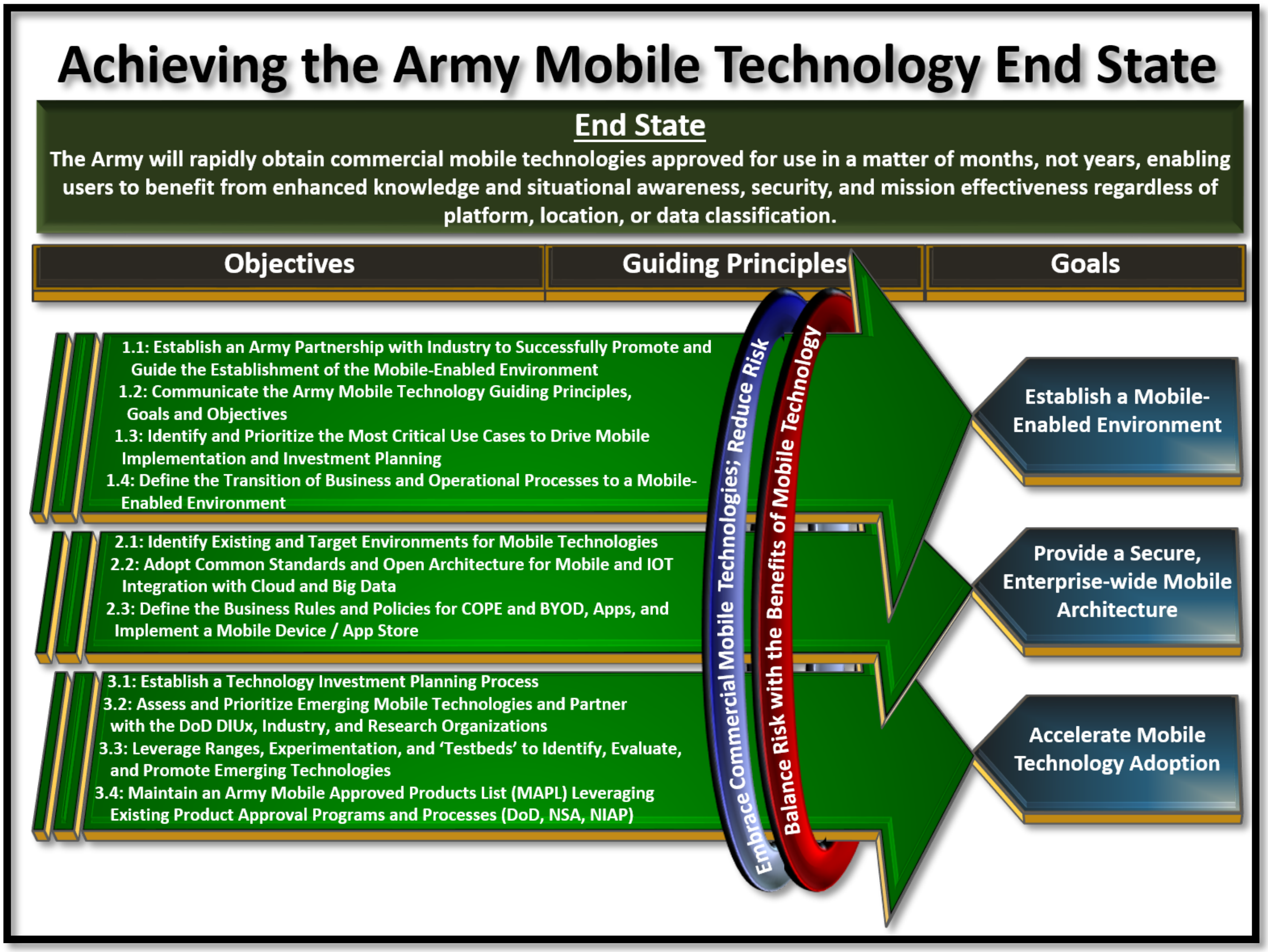
This document is also informed by current and evolving Department of Defense (DoD) strategies and Army operational concepts, listed in Appendix 2.

Strategy for Achieving the Army Mobile Technology End State

Goals, objectives, and associated key activities that are necessary to successfully achieve the Army Mobile Technology End State are defined below:

- **Goal 1: Establish a Mobile-Enabled Environment**
- **Goal 2: Provide a Secure, Enterprise-wide Mobile Architecture**
- **Goal 3: Accelerate Mobile Technology Adoption**

Each goal represents an important outcome that must be achieved for the Army Mobile Technology End State to be successful. Within each goal, objectives and associated key activities represent discrete, measurable ways to assess progress towards the desired end state.



Achieving the Army Mobile Technology End State

End State

The Army will rapidly obtain commercial mobile technologies approved for use in a matter of months, not years, enabling users to benefit from enhanced knowledge and situational awareness, security, and mission effectiveness regardless of platform, location, or data classification.

Objectives	Guiding Principles	Goals
1.1: Establish an Army Partnership with Industry to Successfully Promote and Guide the Establishment of the Mobile-Enabled Environment 1.2: Communicate the Army Mobile Technology Guiding Principles, Goals and Objectives 1.3: Identify and Prioritize the Most Critical Use Cases to Drive Mobile Implementation and Investment Planning 1.4: Define the Transition of Business and Operational Processes to a Mobile-Enabled Environment		Establish a Mobile-Enabled Environment
2.1: Identify Existing and Target Environments for Mobile Technologies 2.2: Adopt Common Standards and Open Architecture for Mobile and IOT Integration with Cloud and Big Data 2.3: Define the Business Rules and Policies for COPE and BYOD, Apps, and Implement a Mobile Device / App Store		Provide a Secure, Enterprise-wide Mobile Architecture
3.1: Establish a Technology Investment Planning Process 3.2: Assess and Prioritize Emerging Mobile Technologies and Partner with the DoD DIUx, Industry, and Research Organizations 3.3: Leverage Ranges, Experimentation, and 'Testbeds' to Identify, Evaluate, and Promote Emerging Technologies 3.4: Maintain an Army Mobile Approved Products List (MAPL) Leveraging Existing Product Approval Programs and Processes (DoD, NSA, NIAP)		Accelerate Mobile Technology Adoption

Embrace Commercial Mobile Technologies; Reduce Risk
Balance Risk with the Benefits of Mobile Technology

Figure 1 – Achieving the Army Mobile Technology End State

Goal 1 Establish a Mobile-Enabled Environment

The Army will establish a mobile-enabled environment to address digital transformation, user experience, security, business enablement, and improved Agile and Development and Operations practices.

To achieve the transformational benefits of mobile technologies, the Army must modify its approach to adopting and implementing mobile technologies and stand up an Army-wide mobile technology program. The CIO/G-6 has engaged key stakeholders across the Army and commercial industry partners to identify a critical set of use cases and lessons learned to drive priority areas of emphasis towards the implementation of mobile technologies across the Army. These engagements are intended to ensure user satisfaction and leverage these stakeholders as a valuable source of innovation. The Army must address personnel and organizational business processes as well as operational processes that can – and must – be modified to gain the benefits of mobile technologies.

Objective 1.1 Establish an Army Mobile Technology Partnership with Industry to Successfully Promote and Guide the Establishment of the Mobile-Enabled Environment

This Army Mobile Technology Partnership will promote and guide the development of the mobile infrastructure, and guide the development and adoption of mobile apps to ensure consistency and commitment to the user experience. Users and developers must have a forum to address needs, requirements, concerns, challenges, and successes so that the Army can quickly and effectively transition to a truly mobile force. This Partnership will support linking with core Army requirements, resourcing, and acquisition processes to bring about the changes proposed in this document.

Key Activities:

1. Identify key use cases that can be augmented by the use of current and emerging mobile technologies (e.g. sensors, robotics, wearable sensors, UAVs, UGVs, etc.) and can meet defined security requirements.
2. Document and prioritize selected processes and functions that can be effectively executed using mobile apps.
3. Implement a risk-based approach to maintain cyber readiness for mobile environments.

Objective 1.2 Communicate the Army Mobile Technology Guiding Principles, Goals and Objectives

Develop and implement a communications outreach and engagement program to educate and inform key stakeholder groups. Engage Army leadership to broaden the understanding and commitment to implementation of the mobile-enabled environment.

Key Activities:

1. Engage key Army leaders and stakeholders with the greatest potential impact on the establishment of a mobile-enabled environment to develop core messages and platforms to optimize the communication of this effort.

Objective 1.3 Identify and Prioritize the Most Critical Use Cases to Drive Mobile Implementation and Investment Planning.

Analyze and review use case data from key stakeholders, and expand that research across the Army to identify the most critical required mobile capabilities for the Army. Perform a risk assessment associated with implementation of each defined capability.

Key Activities:

1. Conduct continuous research, compilation, and assessment of mobile use cases and articulation of target users.
2. Develop a streamlined process for identification and validation of use cases in conjunction with US Army Training and Doctrine Command (TRADOC), Army G-3/5/7, the Communications-Electronics Research Development and Engineering Center and Assistant Secretary of the Army (Acquisition, Logistics and Technology) requirements documentation procedures.

Objective 1.4 Define the Transition of Business and Operational Processes to a Mobile-Enabled Environment.

Many business and operational processes can be improved with mobile technology. It is important to assess key processes and determine where mobile capabilities can be implemented to improve performance and/or user satisfaction. Each major business and operational system and process functional proponent (e.g. financial, HR, acquisition, facilities and infrastructure, education and training, medical, intelligence, etc.) will be engaged to assess the processes and practices within each of the identified primary systems that can be transitioned to mobile capabilities.

Key Activities:

1. Develop a prioritized list of processes and operations that can be improved by current and emerging mobile technologies (e.g. sensors, robotics, wearable sensors, UAVs, UGVs, etc.).

Goal 2 Provide a Secure Enterprise-wide Mobile Architecture

The Army will provide a secure, enterprise-wide mobile architecture and supporting services that enable authorized users context-aware access to data anytime and from any authorized device. Mobile technologies offer unique features and introduce cybersecurity risks which must be addressed. It is critical to understand and mitigate threats posed by the increased attack surface, more complex interactions, and threats targeting the unique attributes of mobile devices.

The Army must provide a mobile environment (architecture and supporting services) that supports users' needs and capabilities, and must address the Army's network and device cybersecurity requirements. The Army's mobile environment must support all operations in both classified and unclassified domains, and must be robust enough to function in disaster response environments.

THREAT

Any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

NIST SP 800-30, *Guide for Conducting Risk Assessments*

Objective 2.1 Identify Existing and Target Environments for Mobile Technologies.

The Army must define a target architecture and identify critical technology investments that ensure interoperability. The target architecture should be based on requirements derived from an approved set of use cases, and should support all operational environments.

Key Activities:

1. Document the Army's existing technical architecture.
2. Define target technical architecture alternatives. Consider the following: (1) devices and networks; (2) mobile device management; (3) mobile app distribution; (4) identity and access management; (5) security architecture; (6) software development tools and development standards; (7) backend services and data sources; and (8) existing architecture products available across the Federal Government (e.g. National Security Agency (NSA) Commercial Solutions for Classified).
3. Identify gaps between existing and target architectures.
    a. Identify critical gaps that must be resolved in the near term and gaps that can be deferred to a later date.
    b. Assess risks and mitigation options for each alternative.
    c. Assess each alternative to identify the best candidate.

4. Develop a plan that defines how the Army transitions from its current state to meet its future mobile needs (to include the network).
5. Assess skills required to operate the objective mobile environment, and conduct a continuous assessment of skills needed to maintain the mobile architecture, infrastructure, supporting policies, related standards, and operations.
6. Implement a risk-based approach to support the use of mobile technologies, to include implementation and maintenance of a mobile threat catalogue that is routinely refreshed to track threats to be considered when refining the Army's mobile architecture.
7. Identify offices of primary responsibility as proponents for portions of the mobile environment, and establish procedures to capture stakeholder input to develop programmatic and technical plans to achieve the Army Mobile Technology End State.

Objective 2.2 Adopt Common Standards and Open Architecture for Mobile and IoT Integration with Cloud and Big Data.

The Army must identify a set of stakeholder-accepted standards for data exposure, security, identity and access management, and mobile app development to ensure that all mobile IT that is developed and implemented adheres to enterprise-wide standards. An open architecture, with managed and open application programming interfaces, will help facilitate development across the Army and allow for innovation across the Army and other services.

***Key Activities**:*

1. Identify the standards efforts that are focused on common architecture frameworks for connected systems interoperability and engage in standards groups for the integration of IoT, such as the AllSeen Alliance and the Open Interconnect Consortium.
2. Identify the gaps in current standards and work with DoD to fill these gaps.
3. Define and implement a robust mobile app vetting process.

Objective 2.3 Define the Business Rules and Policies for Corporately Owned Personally Enabled (COPE) and Bring Your Own Device (BYOD), Apps, and Implement a Mobile Device/App Store.

The Army has a strong interest in using a single mobile device for both personal and business purposes in unclassified environments. The Army-owned mobile device is commonly known as COPE. The personally-owned mobile device is commonly known as BYOD.

Key Activities:

1. Develop business operations, policy and technical guidance to enable access to enterprise resources from both Army-owned and personal mobile devices.
2. Implement a risk-based approach to:
    a. Analyze the security of mobile solutions for BYOD by developing and implementing a threat model framework including repeatable test cases.
    b. Provide an assessment of leading commercial mobile products.
    c. Propose a security and privacy-based architecture for securely accessing enterprise resources from mobile devices.

Goal 3 Accelerate Mobile Technology Adoption

The Army must keep pace with rapid commercial innovation by accelerating the identification, prioritization, testing and approval of mobile technologies. The Army must partner with commercial vendors to ensure that Army requirements can be obtained. This partnership can lead to significant benefits to Army operations. Identifying and experimenting with new mobile technologies in the context of Army use cases and operations is critically important to assess and articulate technological benefits in the context of the proposed use. Establishing criteria for assessment and investment prioritization is crucial given limited budgets.

The Army must implement an Army Mobile Approved Products List (MAPL) in conjunction with DoD, NSA, the National Information Assurance Partnership (NIAP), and others to maintain a list of Army-approved mobile products where mobile products, as defined above, include smart phones, sensors, applications, handheld devices, robotics, and wearables.

Objective 3.1 Establish a Technology Investment Planning Process.

Mobile IT has been instrumental in driving the transformation of business processes in the commercial sector and can be a key enabler for Army operations. It is critical to create a business model for mobile technology acquisition and to define an investment plan for mobile technologies that is based on mission needs, technology capabilities and lifecycle costs.

Key Activities:

1. Establish and execute a marketplace surveillance plan across the Federal Government and the commercial sector to identify products and services that can meet the Army's needs with minimal modification.
    a. Conduct market analyses and identify courses of action for key elements of the mobile architecture.
    b. Assess products and services used across the Federal Government for potential Army use (e.g., mobile app store, and app vetting).
    c. Conduct assessments of commercial products and services that satisfy requirements that cannot be satisfied by existing government efforts.
2. Establish strong industry partnerships.
    a. Identify and foster relationships with key industry partners to share the Army's needs and requirements early in the product development lifecycle.

Objective 3.2 Assess and Prioritize Emerging Mobile Technologies and Partner with the DoD Defense Innovation Unit - Experimental (DIUx), Industry, and Research Organizations.

The Army will investigate current and emerging mobile technologies, assess their applicability to achieving the Army's needs and capability requirements as defined in validated use cases. The Mobile Technology Partnership will coordinate and manage the establishment of enabling business processes (e.g. mobile app store, MAPL, etc.) on behalf of the Army.

Key Activities:

1. Partner with Federal agencies (e.g. the DIUx or other similar organizations) to identify and assess new technologies as they are developed.
2. Establish partnerships with industry to communicate the Army's needs.

Objective 3.3 Leverage Ranges, Experimentation, and Testbeds to Identify, Evaluate, and Promote Emerging Technologies.

The Army must leverage existing business processes, facilities, and infrastructure to successfully move towards the Army Mobility End State. Resources should be allocated to the extent available in conjunction with other Army acquisition and developmental programs and initiatives to assess, evaluate, and when appropriate, approve mobile technologies for use by the Army.

Key Activities:

1. Identify the experimentation and evaluation infrastructure that will support and provide testbeds for Army mobile capability testing.
2. Develop an assessment process for commercial mobile technologies that accounts for unique cybersecurity risks.
3. Develop "hackathon" opportunities to engage academia and the public in Army challenges.

Objective 3.4 Maintain an Army Mobile Approved Products List (MAPL) Leveraging Existing Product Approval Programs and Processes (DoD, NSA, NIAP).

The Army must emulate and adapt accelerated mobile technology development and fielding business processes to enable the Army to effectively identify and adopt emerging mobile technologies. A list of approved and accredited products for use across the Army is key to this adaptation. The Army will work with test / evaluation / approval programs within DoD and industry to maximize the approval processes already in place.

Key Activities:

1. As new mobile technologies solutions are identified and assessed, the Army must work to identify the current policies that must be adjusted. Policies must be flexible to enable adoption sooner. The Army must encourage and promote innovative procedures and practices that can be adapted to Army needs in accordance with acquisition guidelines and policies.
2. Establish a mobile technology lifecycle management process for oversight, management and execution of mobile technology identification, assessment, testing, procurement, fielding, sustainment, upgrade, and replacement processes.

Path Forward

Over the next 5 years, emerging mobile technologies will transform how the Army communicates, collaborates, and innovates. These technologies have the potential to significantly impact the Army. Smartphones and tablets are now at a point where their benefits are clear and established and the technology is stable. Incremental advances are expected to continue in the areas of performance, increases in sensor applications (e.g. heart rate, gesture, infrared, barometer), reduced form factors for mobile devices, and context-aware mobile apps which are shifting innovation and control to the edge of the enterprise and empowering end users.

IoT is a significant technological trend that focuses on the integration of digital sensing, computing, and communications capabilities across innumerable devices. These devices include wearables, like smart helmets/uniforms, clothing, and eyewear; and, include biometric sensors, such as fingerprint scanners, heart rate sensors, and gesture sensors. Finally, IoT leverages technologies such as infrared blasters, barometers, and sensors typically found in smartphones such as Global Positioning Systems, lights, gyros, accelerometers, and proximity sensors.

The digital shift to cloud, mobile, and IoT will be a powerful force for business transformation. These technologies will enable new capabilities and services, with app development playing a key role. Network and bandwidth costs will continue to favor apps that use the power and storage of the client device, and the cloud will become the new source of scalable, self-service computing. Apps will be developed to support synchronized use of multiple peripheral devices: multiple screens, wearables, and other display devices (e.g. Ubuntu Touch). The personal computing industry is pushing 2-in-1, tablet-laptop hybrids, such as the Microsoft Surface Pro 4, which offer a laptop mode for hardcore productivity and a tablet mode for browsing. Other solutions include “Chromebook”-style devices that deliver apps ubiquitously from the cloud.

Additional emerging technologies include:

- **Cyber Physical Systems –** Autonomous vehicles such as UAVs or UGVs, robots, smart energy systems, and medical devices as well as distributed robotics.
- **Virtual and Augmented Reality –** Data accessibility to simultaneously see and interact with the virtual world and real world.
- **Mobile Networks –** This includes 5G networks, which loom on the horizon, advances in Long-Term Evolution (LTE), LTE Direct (Device-to-device proximity discovery), and Wi-Fi networks.
- **Smart Buildings and Workplaces –** Advanced collaborative workspaces, screen “casting” (e.g. Google’s Chromecast), and interoperable video teleconferencing capability to any device (Web Real Time Communications).
- **Virtual Private Assistants –** Natural Language Processing and contextual information to anticipate and provide required information.
- **Visible Light Communications (VLC) –** VLC or Light Fidelity systems that can yield transfer rates in the hundreds of megabits per second up to several gigabits per second depending on range and conditions.
- **Additive Manufacturing (3-Dimensional (3D) printing) –** Rapid prototyping and rapid “manufacturing” of devices and components.
- **Ambient Energy Harvesting –** Capturing and storing energy from natural and human sources found within the environment to provide power to wearable devices and devices that are covered under the IoT.
- **Smart Workspaces** – Advances in building automation systems (climate control, lighting, security), and seamless integration of information sharing and display to enhance collaboration.

It is critical that the Army actively establish an enterprise-wide mobile technology program. The following activities are critical enablers to achieving the Army Mobile Technology End State:

- **Establishment of an Army Mobile Technology Partnership with Industry to Guide the Army’s Mobile Transformation:** Establish a centralized Army/Industry Partnership to lead the execution of this Mobile Technology End State. Key responsibilities include prioritization of mobile use cases/business scenarios, user experience, security policies and standards.
- **Mobile Architecture:** Define a secure enterprise-wide mobile architecture.
- **Communications Plan:** Develop and implement a communication, engagement and outreach program to educate and inform Army leadership, key stakeholder groups, and the entire Army

to broaden the understanding and commitment to implementation of the Mobile Technology End State.

- **Strategic Roadmap**: Develop a high-level roadmap (people, process, technology, and security) that identifies key milestones for achieving the Army Mobile Technology End State. The roadmap should align with Army expectations as identified in use cases as well as plot the approach for achieving the goals and key activities in this document
- **Mobile Life Cycle Business Model for Acquisition and Sustainment**: Identify and formalize tailored life-cycle management processes, procedures, and enduring sources of seed money to resource pilots and initiatives which enable accelerated identification, assessment, implementation, sustainment, and termination/replacement of mobile technologies that are agile and adaptable to the shorter life-cycle and evolution of mobile technologies.

Conclusion

The Army must embrace commercially available mobile technologies to become more dynamic, flexible, resilient, and capable of supporting immediate user demand for information and knowledge. Mobile technologies are not limited to smart phones; rather, mobile technologies include sensors, wearables, robotics, handheld devices, and apps that will improve the speed and effectiveness of current business processes and services, and drive innovation and demand for new capabilities. To effectively embrace mobile technologies, the Army must implement a robust risk assessment process to identify the unique risks associated with these technologies.

By taking action on the activities identified in this document, the Army will initiate the steps necessary to achieve the end state, enabling all members of the Army community to perform their missions more effectively than ever before.

Appendix 1: Terms/Glossary

5G	5th Generation
BYOD	Bring Your Own Device
CIO	Chief Information Officer
COPE	Corporately Owned Personally Enabled Device
DIUx	Defense Innovation Unit - Experimental
DoD	Department of Defense
HR	Human Resources
IoT	Internet of Things
IT	Information Technology
LTE	Long-Term Evolution
MAPL	Army Mobile Approved Products List
NIAP	National Information Assurance Partnership
NSA	National Security Agency
TRADOC	U.S. Army Training and Doctrine Command
UAV	Unmanned Aerial Vehicle
UGV	Unmanned Ground Vehicle
VLC	Visual Light Communications

Appendix 2: References

Enterprise Mobility Strategy, Version 1.0, U.S. Army Medical Command, April 2016

Army Network Campaign Plan, Shaping the Army Network 2025-2040, U.S. Army CIO/G-6, March 2016

Army Network Campaign Plan Implementation Guidance, Mid Term, 2018-22, U.S. Army CIO/G-6, February 2016

Army Network Campaign Plan Implementation Guidance, Near Term, 2016-17, U.S. Army CIO/G-6, February 2016

Army Data Strategy, Version 1.0, U.S. Army CIO/G-6, February 2016

Visualizing the Tactical Ground Battlefield in the Year 2050: Workshop Report, U.S. Army Research Laboratory Special Report ARL-SR-0327, June 2015

The Army Vision – Strategic Advantage in a Complex World, U.S. Army, June 2015

The DoD Cyber Strategy, U.S. Department of Defense, April 2015

Army Cloud Computing Strategy, Version 1.0, U.S. Army CIO/G-6, March 2015

Army Network Campaign Plan 2020 and Beyond, U.S. Army CIO/G-6, 6 February 2015

Force 2025 and Beyond: Unified land Operations – Win in a Complex World, U.S. Army Training and Doctrine Command (TRADOC), October 2014

The U.S Army Operating Concept: Win in a Complex World, TRADOC Pamphlet 525-3-1, U.S. Army Training and Doctrine Command (TRADOC), October 2014

National Security Agency Mobility Capability Package (CP), Version 2.3, U.S. National Security Agency, 4 November 2013

Information Management, Army Information Technology, U.S. Army Regulation 25-1, U.S. Army, 25 June 2013

DoD Commercial Mobile Device Implementation Plan, U.S. Department of Defense, 15 February 2013

DoD Mobility Classified Capability – Secret (DMCC-S), http://www.disa.mil/Enterprise-Services/Mobility/DOD-Mobility/DMCC/Secret

DoD Mobility Unclassified Capability (DMUC), http://www.disa.mil/Enterprise-Services/Mobility/DOD-Mobility/DMUC

The Army Capstone Concept (ACC), TRADOC Pam 525-3-019, U.S. Army Training and Doctrine Command (TRADOC), December 2012

Department of the Army General Orders No. 2012-01 (Assignment of Functions and Responsibilities Within Headquarters, Department of the Army), U.S. Army, 11 June 2012.

DoD Mobile Device Strategy, Version 2.2, U.S. Department of Defense, 8 June 2012

http://ciog6.army.mil